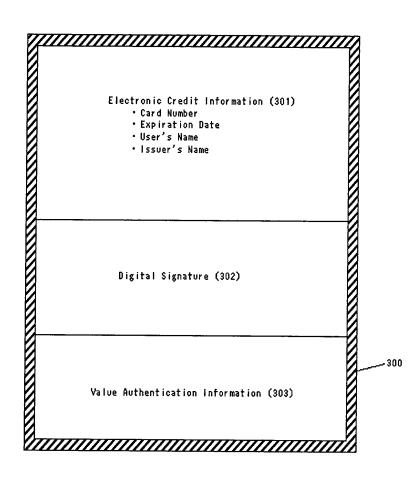
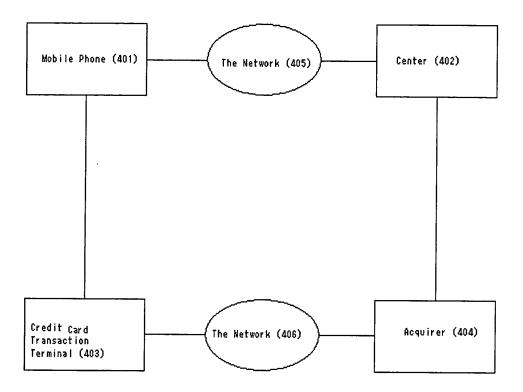
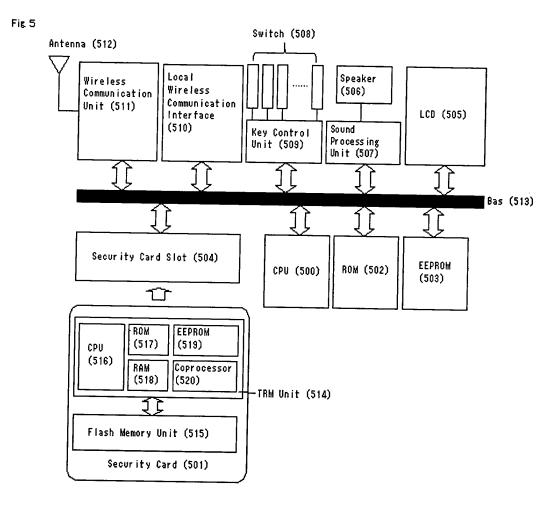


Fig. 3







..

Fig. 6

Card Type #1	Master Key #1	Certificate of Credit Card Issuer #1	Negative List #1	Acquirer Information #1	Risk Management Information #1
Card Type #2	Master Key #2	Certificate of Credit Card Issuer #2	Negative List #2	Acquirer Information #2	Risk Management Information #2
Card Type #3	Master Key #3	Certificate of Credit Card Issuer #3	Negative List #3	Acquirer Information #3	Risk Management Information #3
Card Type #4	Master Key #4	Certificate of Credit Card Issuer #4	Negative List #4	Acquirer Information #4	Risk Management Information #4

Transaction History Information (602)

Flash Memory Unit (515)

Fig. 7

٠<u>.</u>

Wallet Display Information (701) Wallet Sound Information (702)	Wallet Display Information (701)	Wallet Sound Information (702)
---	----------------------------------	--------------------------------

Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Credit #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Credit #3	Property #3

Electronic Credit Public
Information (801)

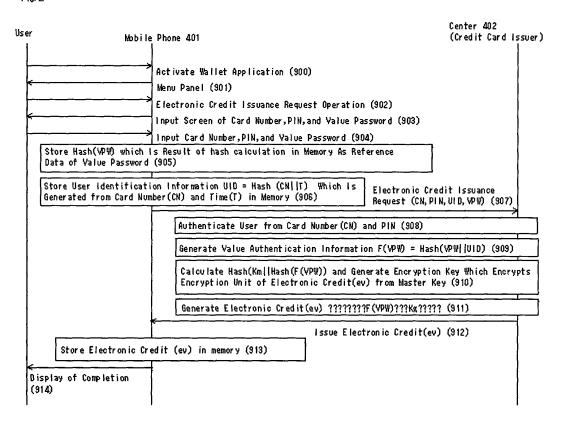
Card Type
Card Number
Expiration Date
User's Name
Issuer's Name

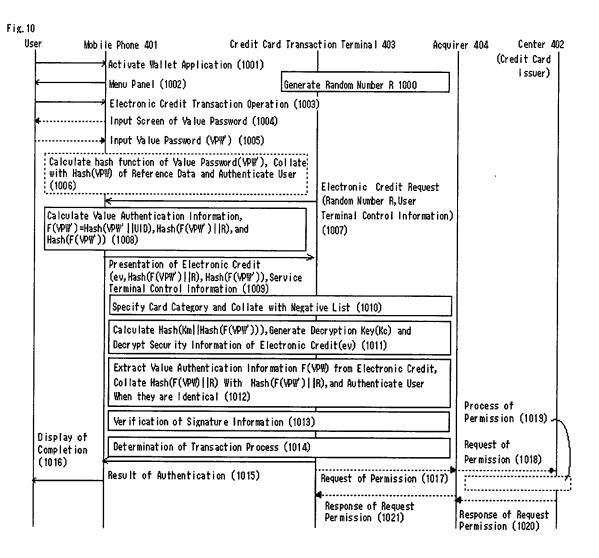
Electronic Credit Secret Information (802)

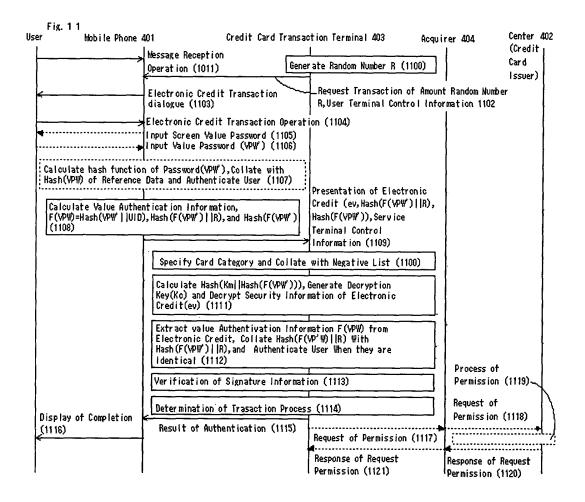
Value Authentication Information (803)

Signature Information (804)

Display Information (805)







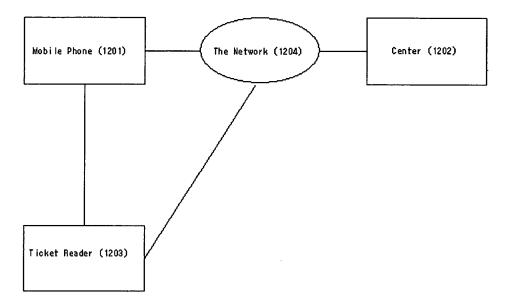


Fig. 13

•

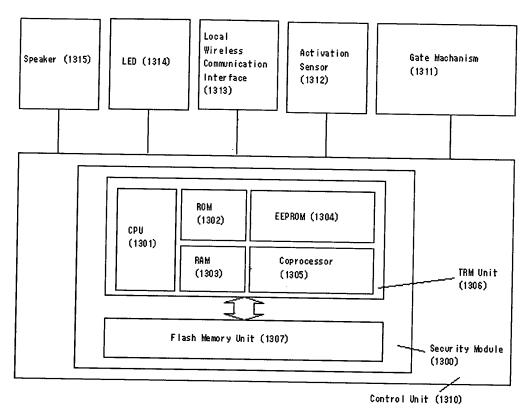


Fig. 1 4

Master Key #1	Certificate of Ticket Issuer #1	Negative List #1
Master Key #2	Certificate of Ticket Issuer #2	Negative List #2
Master Key #3	Certificate of Ticket Issuer #3	Negative List #3
Master Key #4	Certificate of Ticket Issuer #4	Negative List #4
	Electronic Ticket Informat	ion List (1401)
Ticket Booding U	internal defendables (4100)	
	Master Key #2 Master Key #3 Master Key #4	Issuer #1  Master Key #2  Certificate of Ticket Issuer #2  Master Key #3  Certificate of Ticket Issuer #3  Master Key #4  Certificate of Ticket

Flash Memory Unit (1407)

Fig. 15

Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Credit #2	Property #2

Reference Data #1	User Identification Information #1	Electronic Ticket #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Ticket #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Ticket #3	Property #3

Fig. 16

Electronic Ticket Public Information
(1601)

• Ticket Attribute Information
• Expiration Date
• Issuer's Name

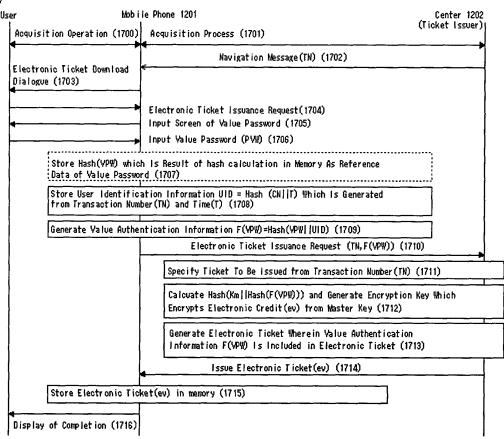
Electronic Ticket Secret Information (1602)

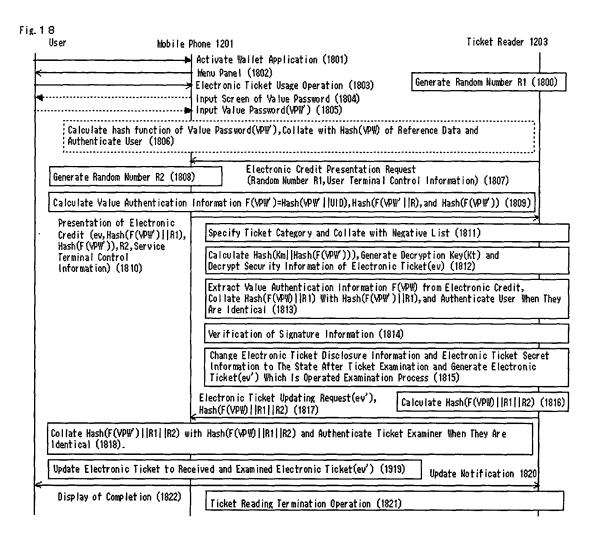
Value Authentication Information (1603)

Signature Information (1604)

Display Information (1605)







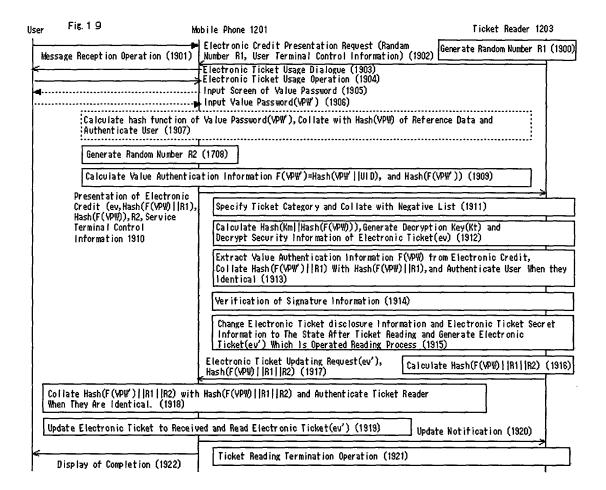


Fig. 20

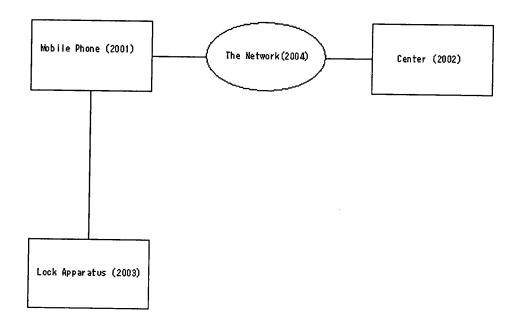
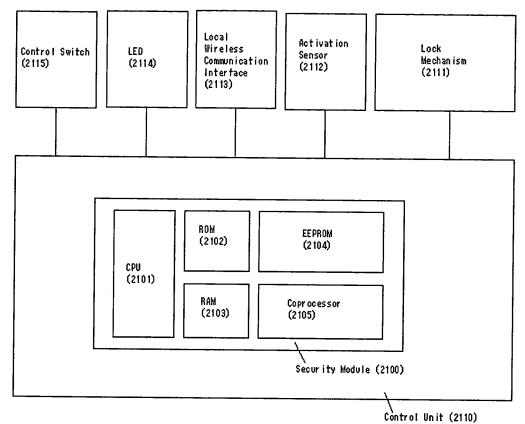


Fig. 21



. .0. -

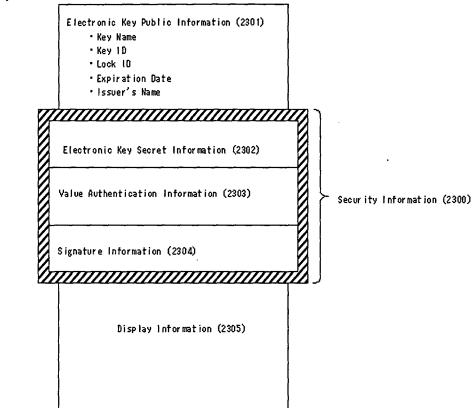
Wallet Display Information (2201)	Wallet Sound Information (2202)

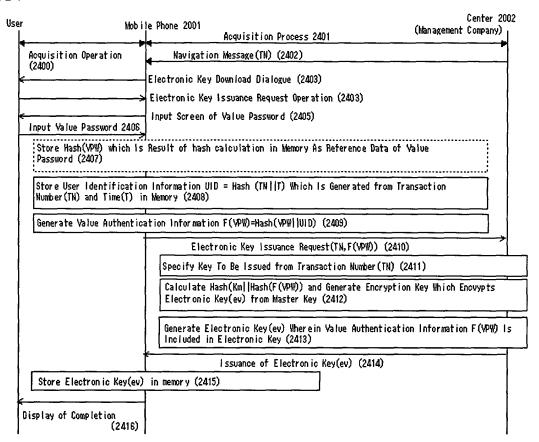
Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
eference Data #2	User Identification Information #2	Electronic Credit #2	Property #2

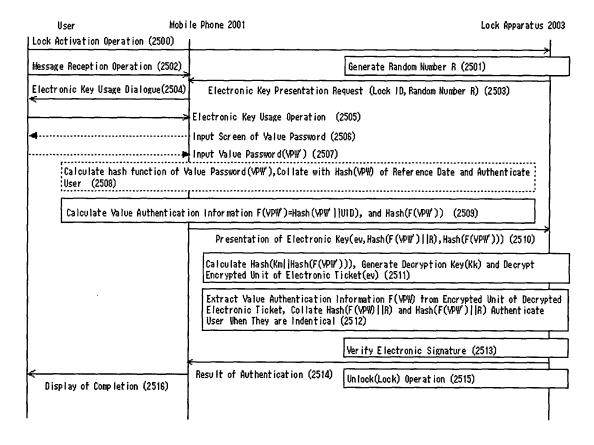
Reference Data #1	User Identification Information #1	Electronic Ticket #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Ticket #2	Property #2

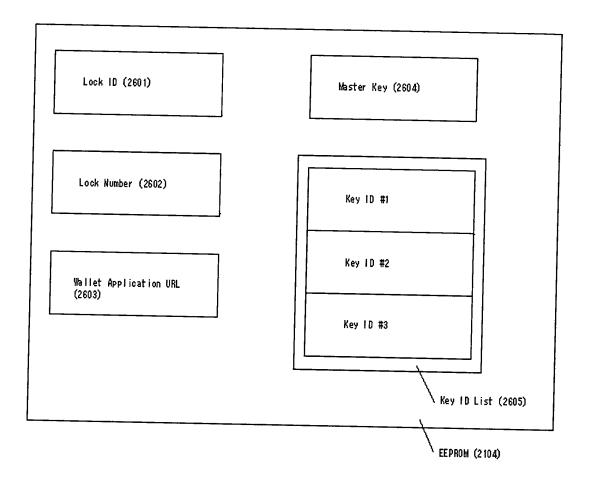
Reference Data #1	User Identification Information #1	Electronic Key #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Key #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Key #3	Property #3

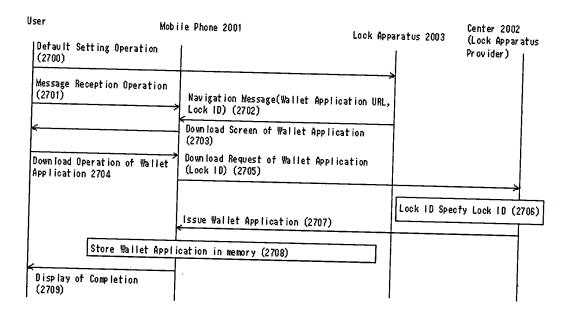


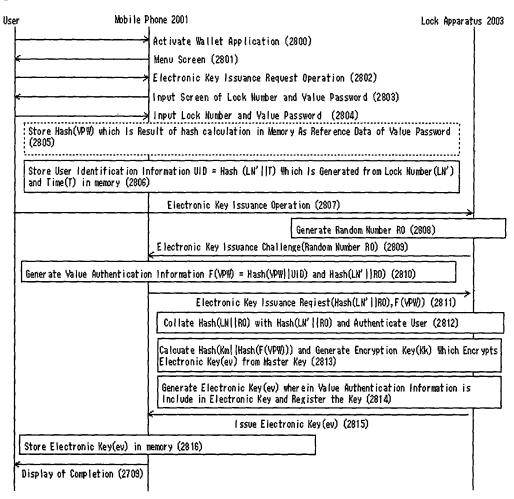


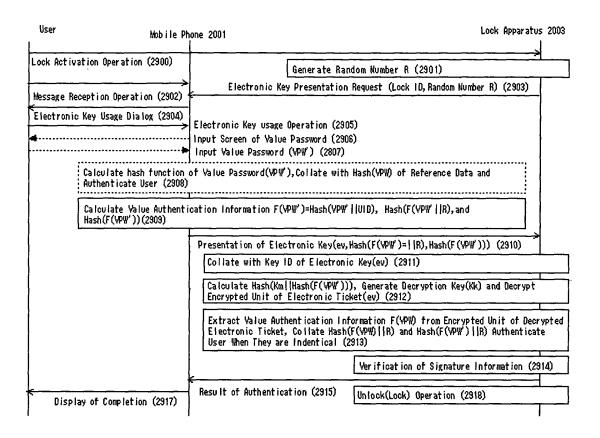












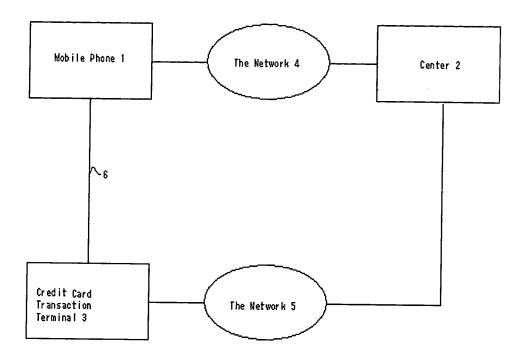


Fig. 3 1

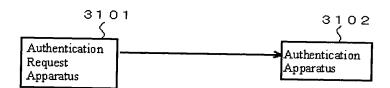
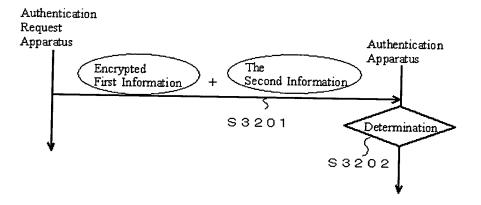


Fig 3 2



## ( A )

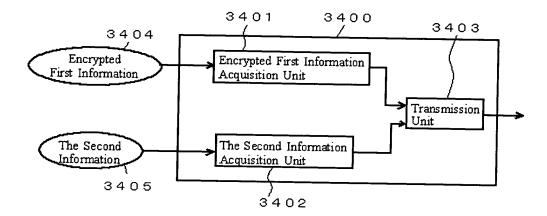
Encrypted First Informaiton	Encrypt ( Password )
The Second Information	Password
Condition of Determination	Decrypt (Encrypted First Information) = The Second Information?

## (B)

Encrypted First Informaiton	Encrypt ( Password )
The Second Information	F ( Password )
Condition of Determination	F ( Decrypt ( Encrypted First Information ) ) = The Second Information?

•

Fig 3 4

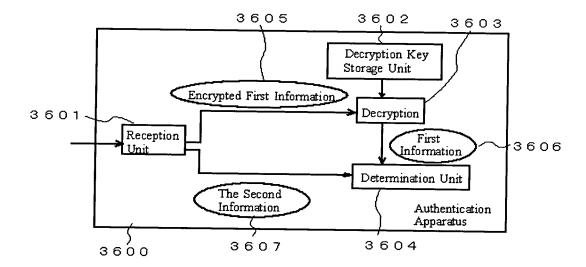


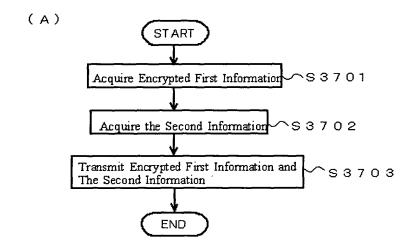
(A)

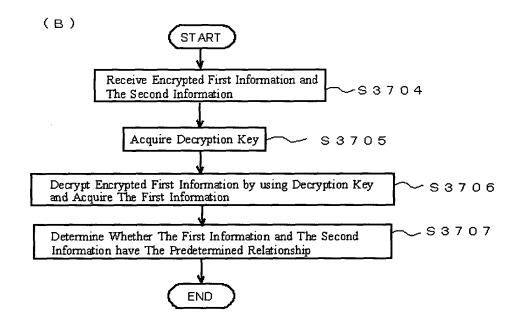
The First Information
Encryption

The First Information + Additional Information

Encryption







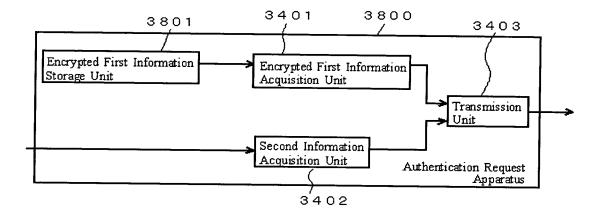


Fig. 3 9

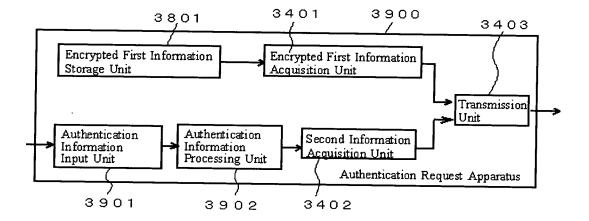
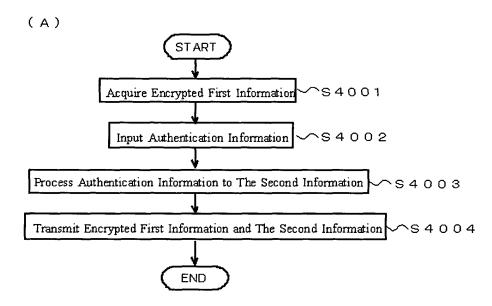
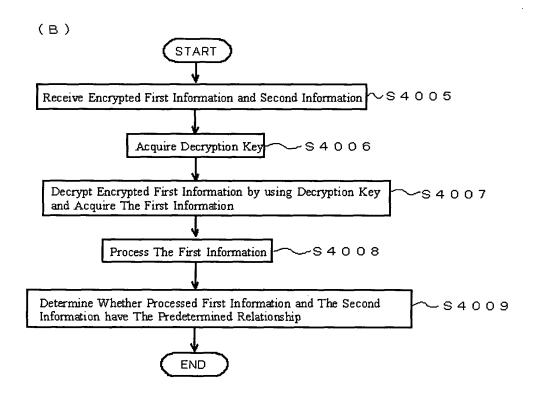
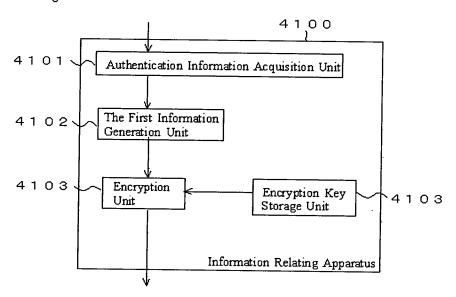


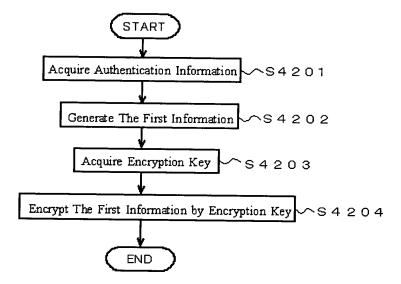
Fig 4 0

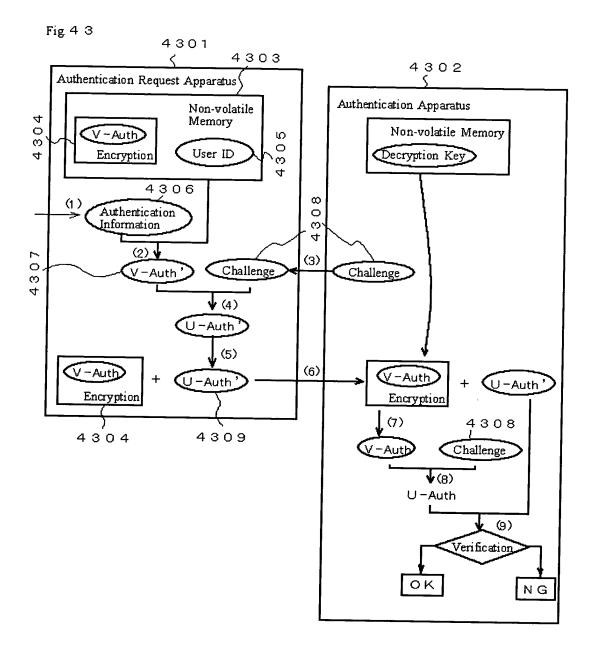












- (1) V-Auth=Hash1 ( Password || User ID)
- (2) V-Auth'=Hash1 (Authentication Information | User ID )
- (3) U-Auth′≡Hash₂(V-Auth′∥ Challenge)
- (4) U-Auth = Hash2 (V-Auth || Challenge)